DISTRIBUTING SYSTEM FOR CRYPTOGRAPHIC KEY

Patent Number: JP62053042
Publication date: 1987-03-07
Inventor(s): KOBAYASHI TETSUJI; others: 01
Applicant(s):: NIPPON TELEGR & TELEPH CORP
Requested Patent: JP62053042
Application Number: JP19850193483 19850902
Priority Number(s):
IPC Classification: H04L9/02 ; G09C1/00
EC Classification:
Equivalents:

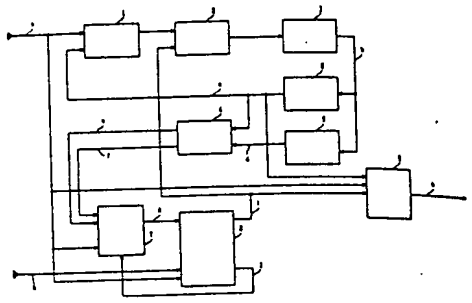
Abstract

PURPOSE:To prevent the effect of the processing speed of an RSA cryptology from being given onto the processing time of the session of the user by separating a key distributed in the RSA cryptology from a key distributed by a DES cryptology.
CONSTITUTION:A data ciphering key distribution key KN is ciphered by the RSA cryptology and distributed by using a public key PK. A data ciphering key KF is ciphered by a DES cryptology and distributed by using the key KN. The keys KN and KF are distributed independently timewise. The master key KM is used within each node to protect other code in each node. The secret key SK is used to decode the RSA cryptology.

(54) **SAMPLING CIRCUIT**
(11) **62-53041 (A)** (43) 7.3.1987 (19) JP
(21) Appl. No. 60-193451 (22) 2.9.1985
(71) NEC CORP (72) TOSHIKI OKUBO
(51) **Int. Cl⁴. H04L7/08,G11B20/10,H03K5/00,H03L7/10,H03L7/18**

PURPOSE: To prevent a phase synchronizing circuit from detecting a synchronizing signal erroneously by using an auxiliary window signal whose window is narrowered more than a reference window signal during the detection of the synchronizing signal so as to sample input information.

CONSTITUTION: An output of a phase detector 1 is connected to a voltage controlled oscillator 3 via an LPF 2. The output of the oscillator 3 is inputted to a reference counter 6 and becomes a reference window signal (c). The signal (c) and the output of an auxiliary counter 5 are inputted to an auxiliary signal circuit 4 to generate auxiliary window signals (e,f). A data discrimination circuit 7 discriminates whether or not the input information (a) is consecutively in the signals (e,f). When the information does not exist in the signals (e,g), a reset signal (g) is outputted. A synchronizing signal detection circuit 8 changes a synchoronization detection signal (i) if the state is consecutive that the specified number of the information (a) and the signal (g) are not inputted.

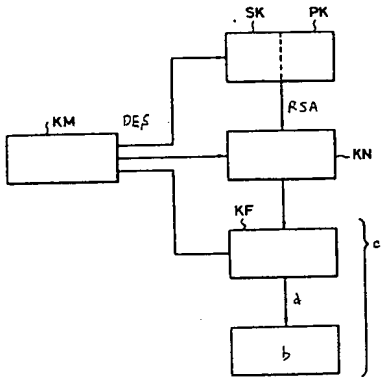


2: low pass filter, b: VOC signal, g: output circuit, k: output data, h: read enable signal, j: enable signal,

(54) **DISTRIBUTING SYSTEM FOR CRYPTOGRAPHIC KEY**
(11) **62-53042 (A)** (43) 7.3.1987 (19) JP
(21) Appl. No. 60-193483 (22) 2.9.1985
(71) NIPPON TELEGR & TELEPH CORP <NTT>
(72) TETSUJI KOBAYASHI(1)
(51) **Int. Cl⁴. H04L9/02,G09C1/00**

PURPOSE: To prevent the effect of the processing speed of an RSA cryptology from being given onto the processing time of the session of the user by separating a key distributed in the RSA cryptology from a key distributed by a DES cryptology.

CONSTITUTION: A data ciphering key distribution key KN is ciphered by the RSA cryptology and distributed by using a public key PK. A data ciphering key KF is ciphered by a DES cryptology and distributed by using the key KN. The keys KN and KF are distributed independently timewise. The master key KM is used within each node to protect other code in each node. The secret key SK is used to decode the RSA cryptology.

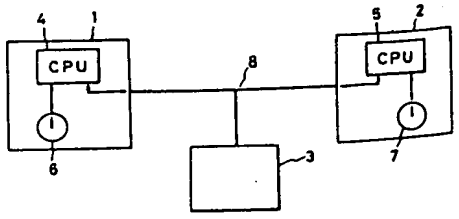


a: usual cryptology by user, b: communication data, c: corresponding to session

(54) **DATA COMMUNICATION CONTROL METHOD**
(11) **62-53043 (A)** (43) 7.3.1987 (19) JP
(21) Appl. No. 60-191854 (22) 2.9.1985
(71) NEC CORP (72) YOSHIHIRO NAKA
(51) **Int. Cl⁴. H04L11/00//H04L13/00**

PURPOSE: To control a data link even a primary station is at fault by allowing each primary station on a data link to set in internal timer every time a data from an opposed primary station is received and establishing the synchronization with respect to the data transmission by the said resetting.

CONSTITUTION: The primary stations 1, 2 exist on the data link 8 and ≧1 secondary station 3 is connected to them. Further, timers 6, 7 and CPUs 4, 5 controlling the timers and data transmission exist in the stations 1, 2. When the timer 6 in the station 1 applies triggering to the CPU 4, the CPU 4 resets Tsec to the timer 6 and starts transmitting a synchronizing data to the data link 8. When the station 2 confirms the data from the station 1, the timer 7 is set to T/2sec. Thus, since the sending of the station 2 is started after T/2sec from the point of time, the station 1 applied transfer control as the primary station during the time.



⑲日本国特許庁(JP)　⑩特許出願公開

⑫公開特許公報(A)　昭62-53042

⑤1Int.Cl.⁴	識別記号	庁内整理番号	④3公開　昭和62年(1987)3月7日
H 04 L 9/02		A-7240-5K	
G 09 C 1/00		7368-5B	

審査請求　未請求　発明の数 1　(全7頁)

⑤4発明の名称　暗号鍵の配送方式

②1特　願　昭60-193483

②2出　願　昭60(1985)9月2日

特許法第30条第1項適用　昭和60年3月5日　社団法人電子通信学会発行の「昭和60年度電子通信学会総合全国大会講演論文集(分冊8)」に発表

⑦2発明者　小林　哲二　横須賀市武1丁目2356番地　日本電信電話株式会社横須賀電気通信研究所内

⑦2発明者　太田　和夫　横須賀市武1丁目2356番地　日本電信電話株式会社横須賀電気通信研究所内

⑦1出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号

⑦4代理人　弁理士　鈴江　武彦　外2名

明　細　書

1.発明の名称

暗号鍵の配送方式

2.特許請求の範囲

複数の情報処理装置間で通信回線により通信を行うシステムにおいて、通信データを暗号化して通信を行うための暗号鍵(暗号化または復号化のために使用する鍵を意味する)の情報処理装置間における配送を、RSA暗号とDES暗号の暗号化装置および復号化装置を用い、且つ暗号鍵の種類として、DES暗号の鍵としては、データ暗号化鍵(通信データを保護するために任意に選択される慣用暗号の暗号鍵)を保護するための鍵である"データ暗号化鍵配送鍵"を用い、RSA暗号の鍵としてはデータ暗号化鍵配送鍵を保護するための鍵である、"データ暗号化鍵配送鍵配送用鍵"を用い、且つ暗号鍵の配送のための通信の処理手順として、データ暗号化鍵の配送にはデータ暗号化鍵配送鍵を鍵とする暗号化と復号化、データ暗号化鍵配送鍵の配送にはデータ暗号化鍵配送鍵配送用鍵を鍵とする暗号化と復号化を用いて行うことを特徴とする暗号鍵の配送方式。

3.発明の詳細な説明

〔発明の技術分野〕

本発明は、通信回線により通信を行う複数の情報処理装置間で、通信の安全性を高めるために、通信データを暗号化して通信を行う際の暗号鍵の配送方式に関するものである。

〔発明の技術的背景とその問題点〕

通信システムにおける複数の情報処理装置(端末、又はセンタであり、以後はノードと呼ぶことがある)の間の通信に暗号化を適用する際は、暗号鍵(以後、単に鍵と呼ぶことがある)をノード間で配送する必要がある。

暗号法は、慣用暗号系と公開鍵暗号系に区分できることが知られている。従来の暗号鍵の配送方式としては、慣用暗号〔例えば、DES暗号("Data Encryption Standard" Federal Information Processing Standards Publication

46, 1977, USA)、など〕による方式〔例えば、SNA方式(R.E. Lennon " Cryptography Architecture for Information Security ", IBM Systems Journal, Vol. 17, 点2 ,pp.138-151 , (1978))、又は、DCNA方式(日本電信電話公社 " DCNA ネットワーク管理プロトコル", 日本データ通信協会, (1981) など〕と、公開鍵暗号〔例えば、RSA暗号(Rivest, R.L. et al. " A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol. 21, 点2 , pp. 120-126,(1978) など〕による方式〔MIX方式(一松信(監修) " データ保護と暗号化の研究 ", 日本経済新聞社, (1983) など〕が提案されている。

従来の方式の問題点は、次のとおりである。慣用暗号による鍵配送方式では、通信データの暗号用の鍵は、鍵配送用の鍵で暗号化して配送できるが、ノード間の鍵配送用の鍵は、事前に人手により秘密に配送する必要があるのが、操作性と安全性の点から欠点である。公開鍵暗号による鍵配送方式は、鍵配送にのみ公開鍵暗号を用いても、慣用暗号による鍵配送方式よりも処理速度が遅いのが欠点である。

〔発明の目的〕

本発明の目的は、RSA暗号を利用することにより人手による鍵の配送を不要として鍵配送の操作性を高め、かつ鍵配送の処理速度に関しては、鍵に複数の種類を設けることにより、利用者の処理時点ではRSA暗号の処理時間の影響がないようにすることにより、従来の各方式の問題点を解決した、暗号鍵の配送方式を提供することである。

〔発明の概要〕

本発明は、RSA暗号を用いることにより、鍵の配送に人手の介在を不要とし、且つ、RSA暗号で配送する鍵と、DES暗号で配送する鍵とを、鍵に複数の種類を設けることによって分離することにより、RSA暗号の処理速度が、利用者のセッション(通信処理の単位)の処理時間に影響を与えないようにした鍵の配送方式である。従来の技術とは、鍵配送にRSA暗号とDES暗号を用いること、鍵の種類、及び鍵の配送のための通信の処理手順において、異なっている。

〔発明の実施例〕

次の種類の暗号鍵を設ける。

(a) マスタ鍵：KMと表す。各ノード内に閉じて使用し、他の鍵をノード内で保護するために用いる。DES暗号の鍵である。各ノードが、それぞれ独立に生成し、それぞれの記憶装置に保存する。

(b) データ暗号化鍵配送鍵：KNと表す。データ暗号化鍵(KF)をノード間で配送する時の保護を行う。DES暗号の鍵である。一対のノードのいずれか一方で生成し、両方のノードで、同じ値の鍵をそれぞれの記憶装置に保存する。

(c) データ暗号化鍵配送鍵配送用鍵：RSA暗号の鍵であり、公開鍵をPK、秘密鍵をSKと表す。データ暗号化鍵配送鍵(KN)をノード間で配送する時の保護を行う。公開鍵は、RSA暗号の暗号化装置に用いる鍵であり、秘密鍵は、RSA暗号の復号化装置に用いる鍵である。公開鍵および秘密鍵は、センタ又は端末で生成し、生成を行ったノードの記憶装置に保存する。

(d) データ暗号化鍵：KFと表す。通信データを保護するための鍵である。セッションの利用者が指定する任意の暗号の種別の暗号の鍵であり、この暗号の種別については、本発明では限定しない。データ暗号化鍵は、一対のノードのいずれか一方で、セッションごとに生成し、両方のノードで、それぞれの記憶装置に保存し、セッションの終了時に両方のノードでそれぞれ廃棄する。

第6図は各鍵の相互関係を示し、矢印は x → y で、x がyの暗号化／復号化に用いられることを表す。

RSA暗号によるPKとSKは、次のとおりである。RSA暗号における平文をM、暗号文をCとすると、

$$C \equiv EXP(M, e) \pmod{n} \quad (1)$$

$$M \equiv EXP(C, d) \pmod{n} \quad (2)$$

である。ここで、任意の整数U，Vについて、EXP(U,V)=U^V と定義する。任意の整数a，b，mについて、aとbがmを法として合同であることを、a≡b (mod m) と表す。式(1)と式(2)において、C，M，e，d，nはいずれも整数である。この場合、eとnがPKであり、dがSKである。n，d，eは、次の式を満たすように選択する。

$$n = p \cdot q \quad (3)$$

$$GCD\{d,(p-1)(q-1)\} = 1 \quad (4)$$

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)} \quad (5)$$

式(3)，式(4)および式(5)において、p，qは互に異なる素数であり、GCD{K,L}は、任意の整数KとLについての最大公約数である。

暗号化は暗号化装置で行い、復号化は復号化装置で行う。暗号化装置と復号化装置の機能を、次の関数で表す。すなわち、E(x;y)を、任意の情報yを鍵xにより、鍵xの暗号法で暗号化した値とする。D(z;w)を、任意の情報wを鍵zにより、鍵zの暗号法で復号化した値とする。暗号法としては、RSA暗号，DES暗号、及びこれら以外の暗号法がある。乱数の発生は、乱数発生器により行う。暗号化装置、復号化装置、及び乱数発生器は、情報処理装置とは独立した装置とすることも、情報処理装置の一部分とすることも可能である。また、これらの装置は、ハードウエア、ソフトウエア、又はハードウエアとソフトウエアの組み合わせにより構成する。

即ち、第1図(a)はDES暗号による暗号化装置Jの変換機能の説明図であり、任意の入力情報yを鍵xにより、鍵xの暗号法で暗号化して出力情報E(x;y)を得る。第1図(b)はDES暗号による復号化装置Zの変換機能の説明図であり、任意の入力情報wを鍵zにより、鍵zの暗号法で復号化して出力情報D(z;w)を得る。第2図(a)はRSA暗号による暗号化装置Jの変換機能の説明図であり、任意の入力情報yを鍵PKにより、鍵PKの暗号法で暗号化して出力情報E(PK;y)を得る。第2図(b)はRSA暗号による復号化装置Iの変換機能の説明図であり、任意の入力情報wを鍵SKにより、鍵SKの暗号法で暗号化して出力情報D(SK;w)を得る。

鍵の配送法は次のとおりである。即ち、第6図に示すようにKNは、PKによりRSA暗号で暗号化して配送する。KFは、KNによりDES暗号で暗号化して配送する。KNの配送とKFの配送とは、時間的に独立に行うことができる。また、どのノードもKN又はKFの配送処理の手順を開始することが可能である。各ノードには、そのノードを一意に識別できるノード識別情報UI(Iは、ノード名称)を付与する。任意のノードは、他のノードのノード識別情報を知ることができる。

通信を開始する二つのノードの名称をAとBとし、ノードAはデータ暗号化鍵配送鍵配送用鍵は無し、ノードBはデータ暗号化鍵配送鍵配送用鍵が有りとする。ノードの名称AとBは、任意の名称でよい。ノードAとノードBは、別のノードである。PKbとSKbを、それぞれノードBの公開鍵と秘密鍵とし、通信の開始前にノードBで設定済とする。KMaとKMbを、それぞれノードAとノードBのマスタ鍵とし、通信の開始前に各ノードで設定済とする。ノードAとノードBで共有するKNを、KNabとする。

この場合にノードAからKNの配送処理を開始する手順の例を、手順1に示す。また、ノードBからKNの配送処理を開始する手順は、手順1の一部分を使用するものであり、手順2に示す。KNの配送は、利用者のセッションとは独立に行うことができる。

(手順1) ノードAからKNの配送処理を開始する手順を第3図を参照して説明する。

ステップ(Step) 1：ノードAは、ノードBにPKの配送要求を含む電文301を送信する。その後で、ノードAはKNabを乱数発生器により生成し、E(KMa;KNab)をノードAの記憶装置に保存する。

Step 2：ノードBは、ノードAからPKの配送要求を受信すると、ノードAにPKbを含む電文

302を送信する。

Step 3 ：ノードAは、ノードBからPKbを受信すると、E(PKb ; KNab ⊙ Ua)を含む電文303をノードBに送信する。(⊙は、連結(二つ以上のデータをそのままの位で結合すること)を表す。Uaは、ノードAの識別情報を表す。)

Step 4 ：ノードBは、ノードAからE(PKb ; KNab ⊙ Ua)を受信すると、鍵SKbにより復号化し、KNabを得る。そして、E(KMb ; KNab)をノードBの記憶装置に保存する。

(手順2) ノードBからKNの配送処理を開始する手順を第4図を参照して説明する。

Step 1 ：ノードBは、ノードAにPKbを含む電文401を送信する。

Step 2 ：ノードAは、ノードBからPKbを受信すると、KNabを乱数発生器により生成し、E(KMa ; KNab)をノードAの記憶装置に保存する。そして、E(PKb ; KNab ⊙ Ua)を含む電文402をノードBに送信する。

Step 3 ：ノードBは、ノードAからE(PKb ; KNab ⊙ Ua)を受信すると、鍵SKbにより復号化し、KNabを得る。そして、E(KMb ; KNab)をノードBの記憶装置に保存する。

次に、ノードA及びノードBは、データ暗号鍵配送鍵配送用鍵は無しとする。ノードCは、データ暗号鍵配送鍵配送用鍵が有りとする。PKcとSKcを、それぞれノードCの公開鍵と秘密鍵とする。ノードA、ノードB及びノードCは、異なるノードとする。ノードBがノードAとセッションを開始する場合には、ノードCからPKとSKの供給を受けることになる。この場合には、KNの配送は手順1と手順2を併用することにより実現できる。この手順の例を手順3に示す。

(手順3)

Step 1 ：ノードBとノードCの間で手順1のStep 1, Step 2, Step 3、及びStep 4を実行する(ノード名称は手順1のノードAとノードBについて、ノードAがノードB、ノードBがノードCに、それぞれ変る。)ことにより、ノードBは、PKcとKNbcを得る。KNbcは、ノードBとノードCで共有するKNである。そして、ノードBは、PKc及びE(KMb ; KNbc)を記憶装置に保持する。

Step 5 ：ノードCは、ノードBにE(KNbc ; SKc ⊕ Uc)を送信する。ノードCは、ノードBにE(KNbc ; SKc ⊕ Uc)を送信後に、ノードCのPKcとSKcを廃棄する。(Ucは、ノードCの識別情報を表す。)

Step 6 ：ノードBは、E(KNbc ; SKc ⊕ Uc)を受信すると、それからSKcを得て、E(KMb ; SKc)を記憶装置に保存する。

Step 7 ：ノードBは、PKc, SKcをそれぞれPKb, SKbと扱うことにより、ノードAに対して、手順2のStep 1, Step 2, 及びStep 3を実行する。

KFの配送処理の手順には、慣用暗号による鍵配送の手順として知られている方法を用いる。その例を手順4に示す。

(手順4) KFの配送処理の手順を第5図を参照して説明する。

I-AXを、データの暗号化のために使用する慣用暗号の種別を指定する情報とする。

Step 1 ：ノードAは、KFabを生成し、E(KMa ; KFab)をノードAの記憶装置に保存する。そして、E(KNab ; KFab ⊙ I-AX ⊙ Ua)を含む電文501をノードBに送信する。

Step 2 ：ノードBは、E(KNab ; KFab ⊙ I-AX ⊙ Ua)からKFabを得て、E(KMb ; KFab)をノードBの記憶装置に保存する。そして、乱数発生器により乱数RNを生成し、RNをノードBの記憶装置に保存する。更に、E(KFab ; RN ⊙ Ub)を含む電文502をノードAに送信する。(Ubは、ノードBの識別情報を表す。)

Step 3 ：ノードAは、E(KFab ; RN ⊙ Ub)からRNを得て、ノードAの記憶装置に保存する。そして、あらかじめ両ノードで定めてある関数f(·)をRNに施すことにより、f(RN) = RN1を得る。更に、E(KFab ; RN1 ⊙ Ua)を含む電文503をノードBに送信する。f(·)は、例えば、一定の

ビット位置のビットの反[redacted]行う関数とする。

Step 4 ：ノードBは、E(KFab ; RN1 ⊙ Ua)からRN1を得て、ノードBで保存していたRNにより f(RN) の演算を行い、RN1と比較する。その結果、f(RN) = RN1となったときは、KFの配送手順を正常終了し、そうでないときにはKFの配送手順を異常終了する。

〔発明の効果〕

(1) 性能上の効果

次の二つの方式の性能比較を行う。

〔方式1〕本発明の実施例の暗号鍵の配送方式。

〔方式2〕KNは使用せずに、KFを直接にRSA法により配送する方式。

一つのセッションについて、暗号通信に伴う二つのノードの処理時間の増加量の和を、方式1，方式2について、それぞれZ1，Z2（通信時間は除いて考える）とすると、

Z1＝DES暗号によるKFの暗号化および復号化時間
＋利用者の暗号（慣用暗号）による通信データの暗号化および復号化時間

Z2＝RSA暗号による[redacted]KFの暗号化および復号時間
＋利用者の暗号（慣用暗号）による通信データの暗号化および復号化時間

故に、本発明の暗号鍵の配送方式では、RSA暗号の処理速度が、利用者のセッションの処理時間に影響しないので、高速な鍵配送システムを構成できる。

(2) 操作性

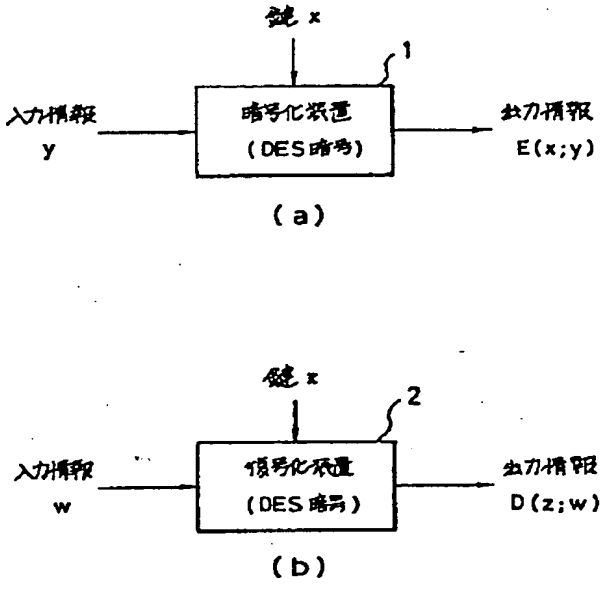
本発明の方式では、鍵の配送に人手の介在は不要である。また、任意のノードから鍵の配送処理を開始できるため、ノードを追加または削除するときの処理が容易である。

以上のように、本発明では、利用者のセッションの処理に公開鍵暗号の処理速度が影響せず、且つ鍵配送に人手の介在は不要である、という利点がある。

4. 図面の簡単な説明

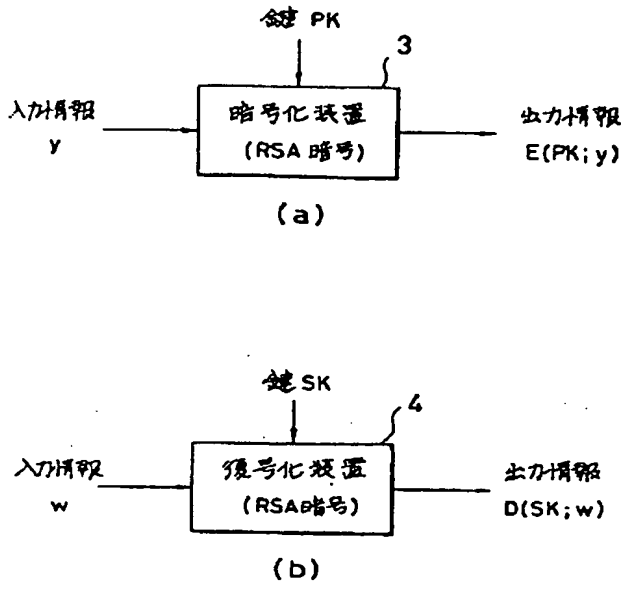
第1図～第6図は本発明の一実施例を説明する図であり、第1図はDES暗号による暗号化装置と復号化装置の変換機能の説明図、第2図はRSA暗号による暗号化装置と復号化装置の変換機能の説明図、第3図はKNの配送の手順（手順1）の説明図、第4図はKNの配送の手順（手順2）の説明図、第5図はKFの配送の手順（手順4）の説明図、第6図は鍵の相互関係の説明図である。

1 …暗号化装置（DES暗号）、2 …復号化装置（DES暗号）、3 …暗号化装置（RSA暗号）、4 …復号化装置（RSA暗号）、301 … " PKの配送要求 " を含む電文、302 … " PKb " を含む電文、303 … " E(PKb ; KNab ⊙ Ua) " を含む電文、401 … " PKb " を含む電文、402 … " E(PKb ; KNab ⊙ Ua) " を含む電文、501 … " E(KNab ; KFab ⊙ I－AX ⊙ Ua) " を含む電文、502 … " E(KFab ; RN ⊙ Ub) " を含む電文、503 … " E(KFab ; RN1 ⊙ Ua) " を含む電文。

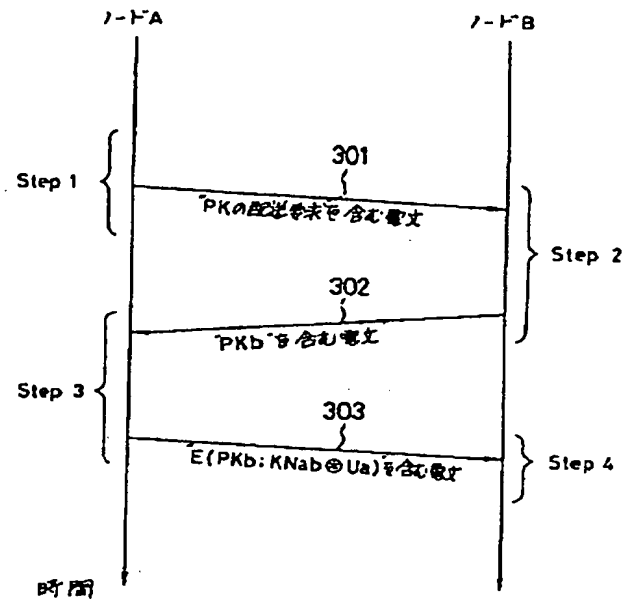


第 1 図

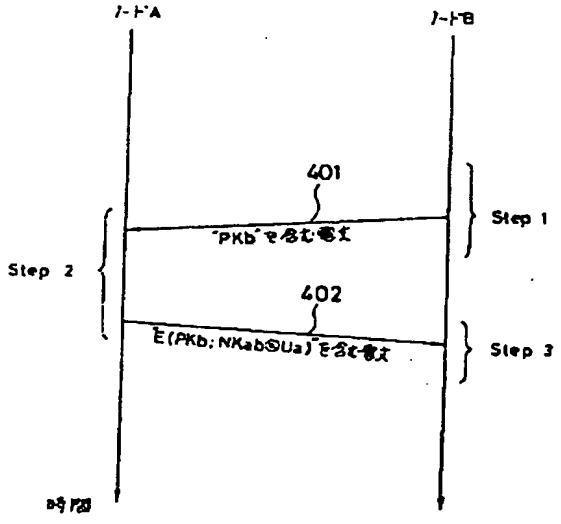
出願人代理人　弁理士　鈴江武彦



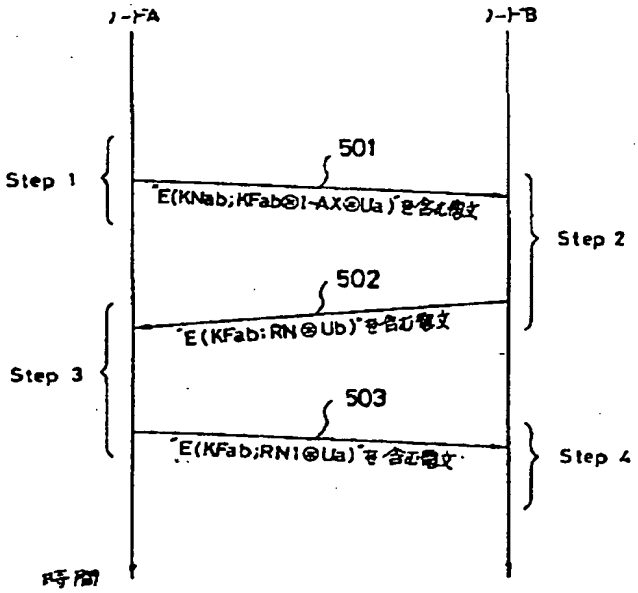
第 2 図



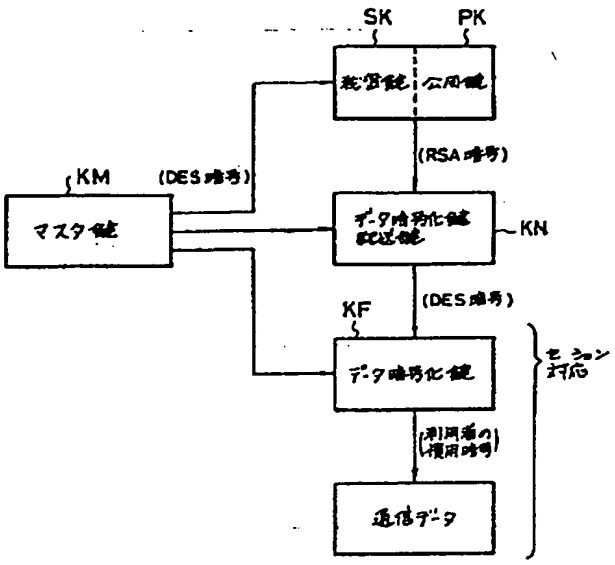
第 3 図



第 4 図



第 5 図


SK
PK
秘密鍵
公開鍵
(RSA暗号)
KM
(DES暗号)
マスタ鍵
データ暗号化鍵
配送鍵
KN
(DES暗号)
KF
データ暗号化鍵
セッション対応
(利用者の情報暗号)
通信データ

第 6 図